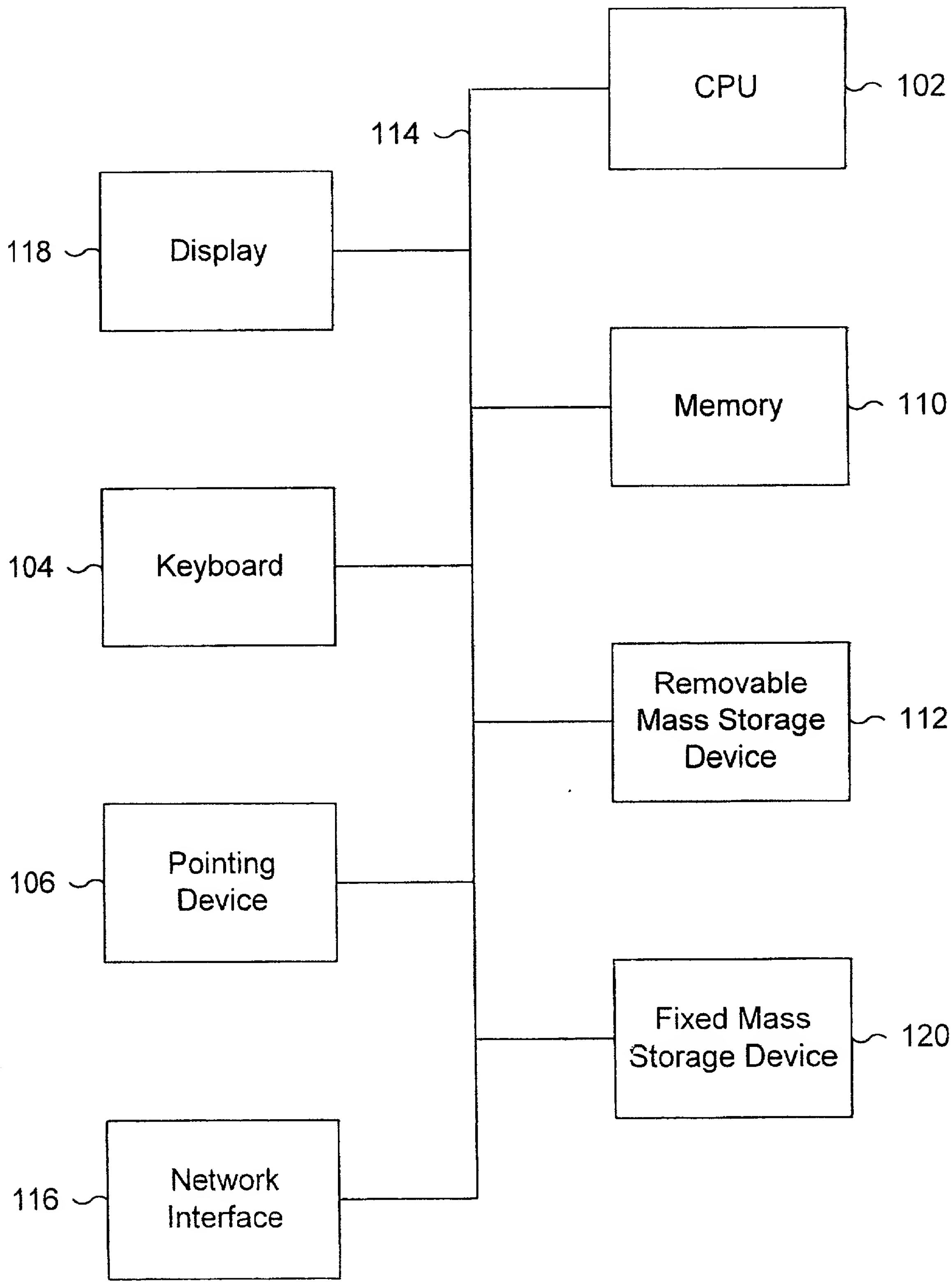
CPU
102
114
Display
118
Memory
110
Keyboard
104
Removable Mass Storage Device
112
Pointing Device
106
Fixed Mass Storage Device
120
Network Interface
116

Figure 1

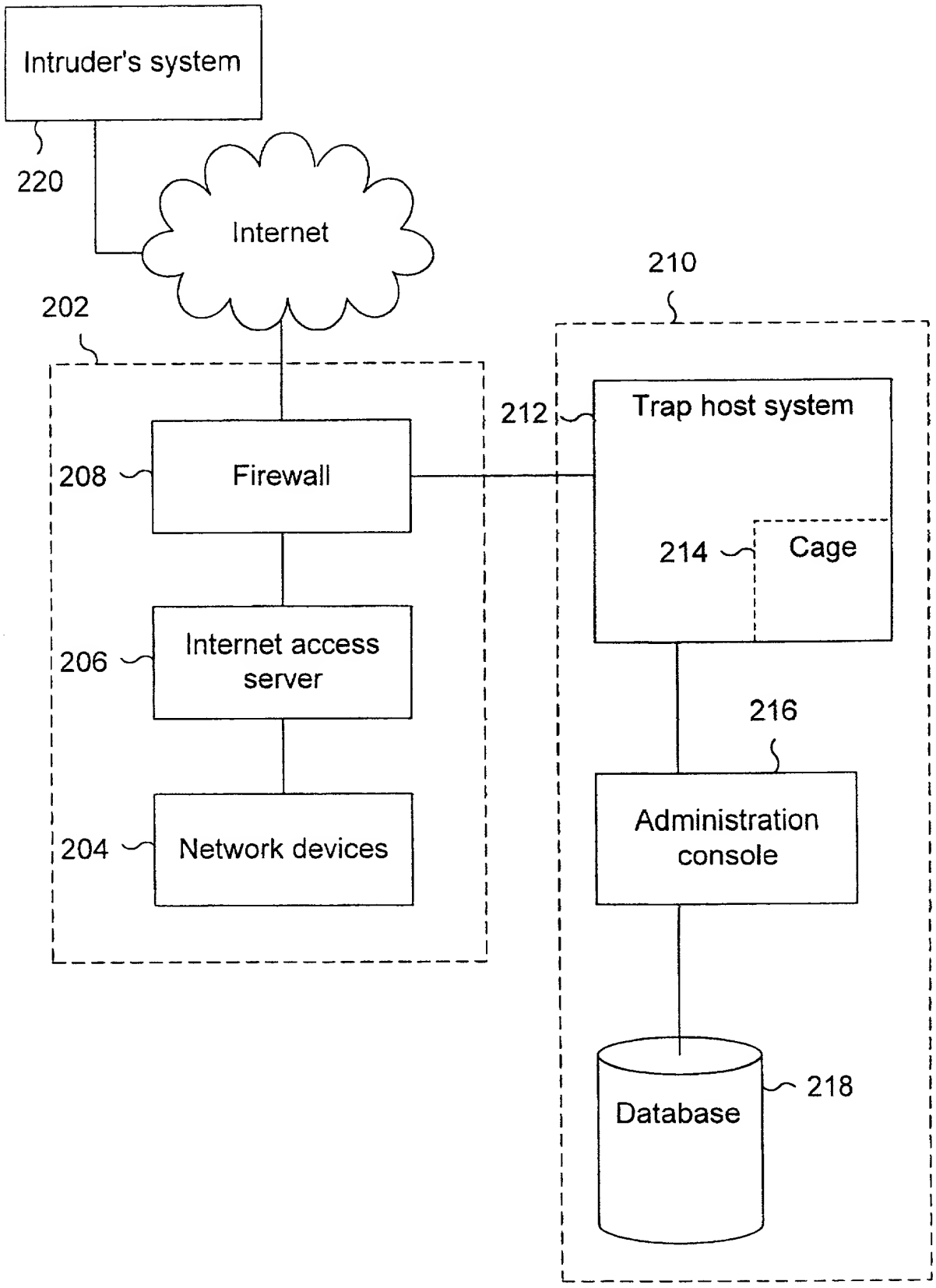
Intruder's system
220
Internet
210
202
212
Trap host system
208
Firewall
214
Cage
206
Internet access server
216
Administration console
204
Network devices
Database
218

Figure 2

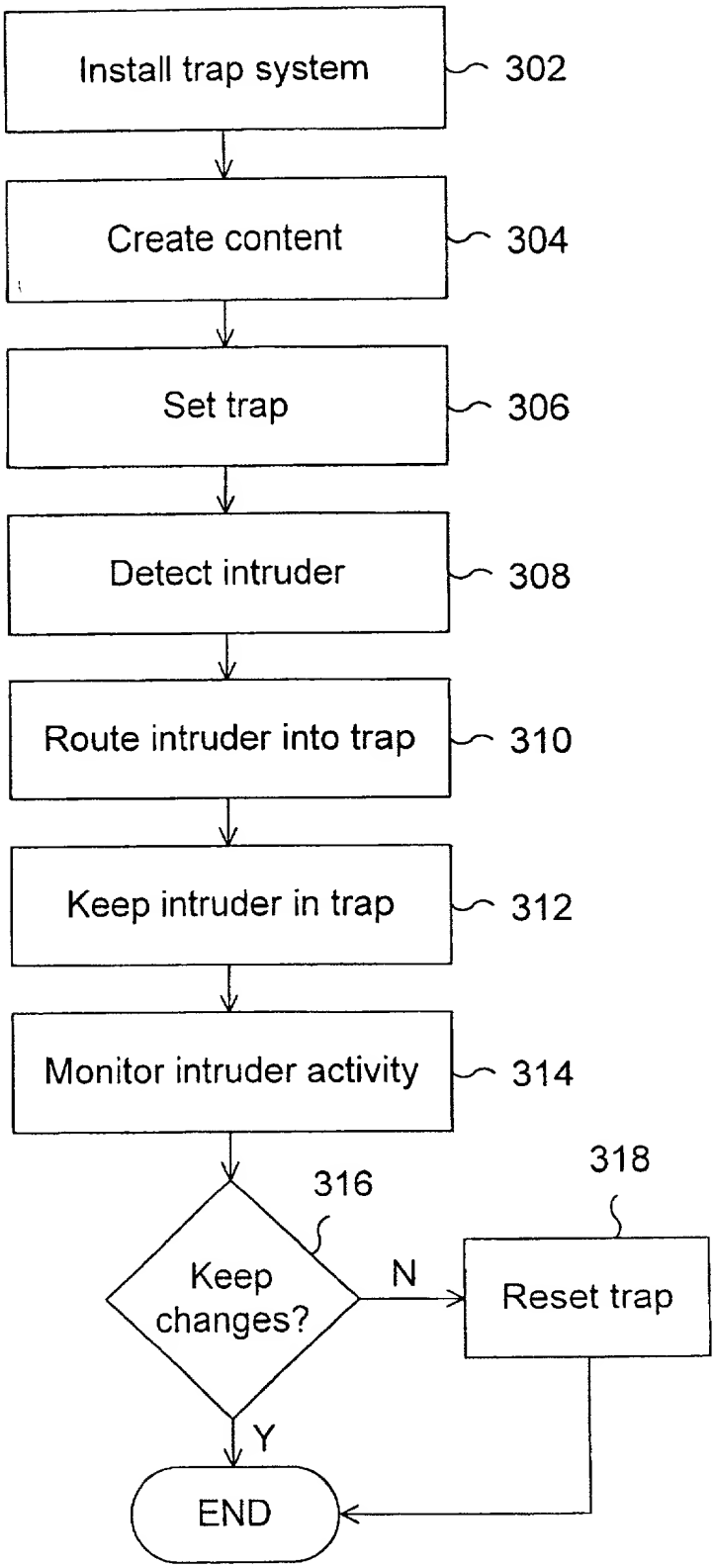
Install trap system
302
Create content
304
Set trap
306
Detect intruder
308
Route intruder into trap
310
Keep intruder in trap
312
Monitor intruder activity
314
316
Keep changes?
N
318
Reset trap
Y
END

Figure 3

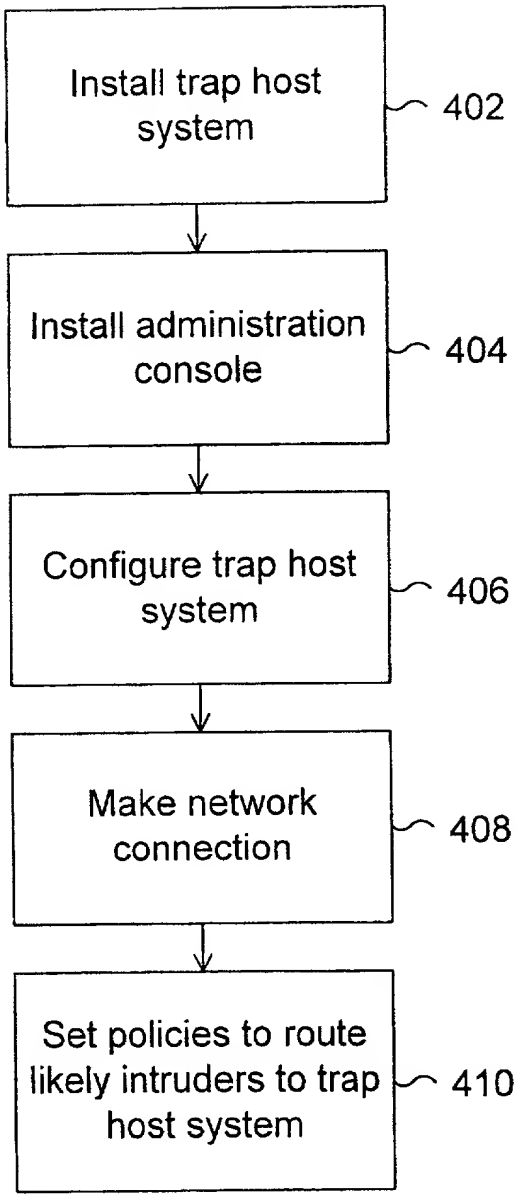
Install trap host system
402
Install administration console
404
Configure trap host system
406
Make network connection
408
Set policies to route likely intruders to trap host system
410

Figure 4

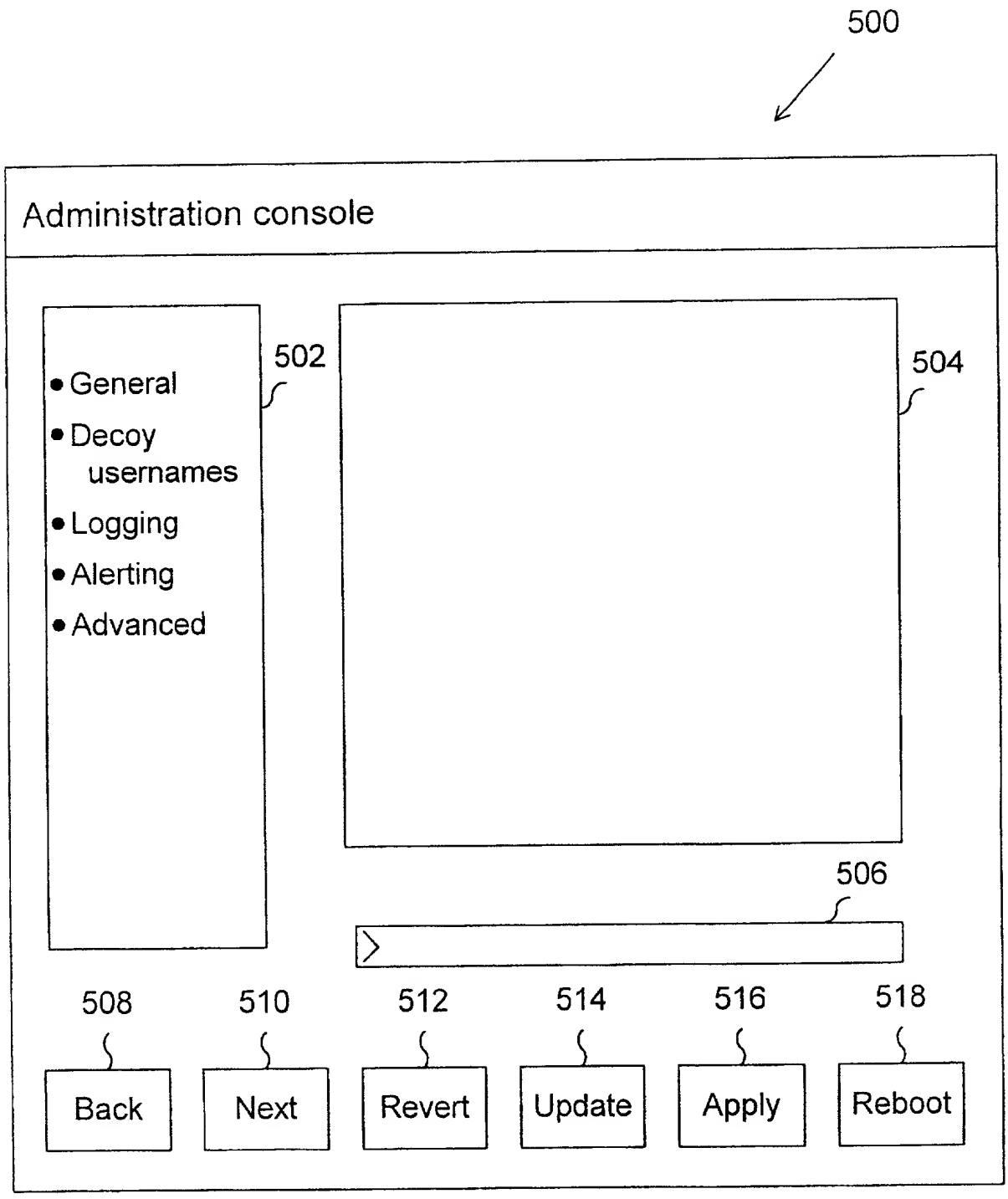
500
Administration console
• General
• Decoy usernames
• Logging
• Alerting
• Advanced
502
504
506
508
510
512
514
516
518
Back
Next
Revert
Update
Apply
Reboot

Figure 5

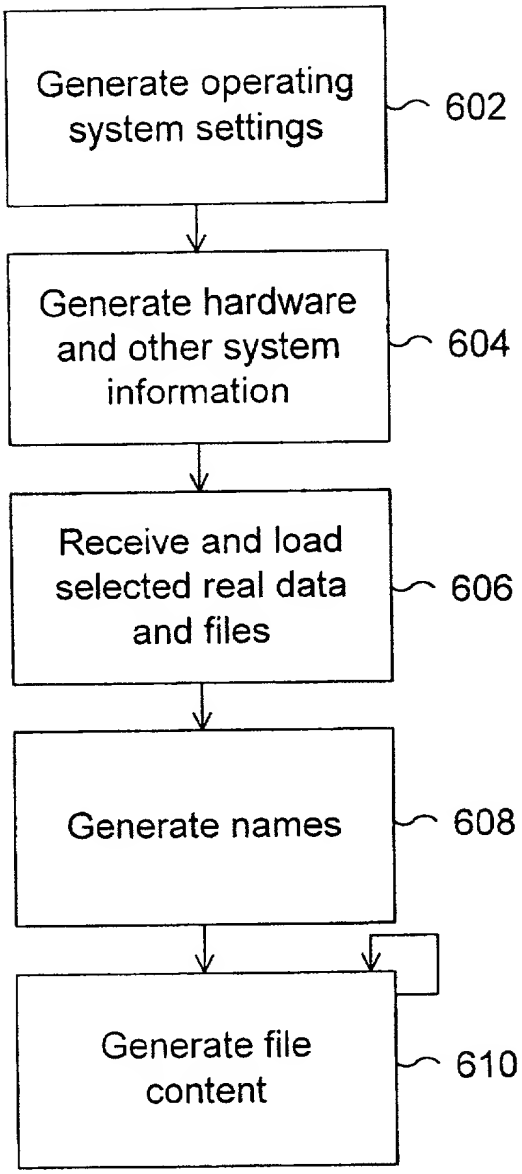
Generate operating system settings
602
Generate hardware and other system information
604
Receive and load selected real data and files
606
Generate names
608
Generate file content
610

Figure 6

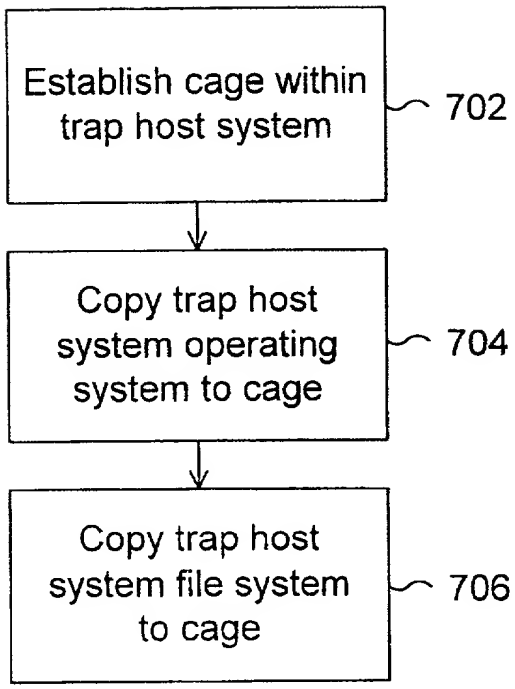
Establish cage within trap host system
702
Copy trap host system operating system to cage
704
Copy trap host system file system to cage
706

Figure 7

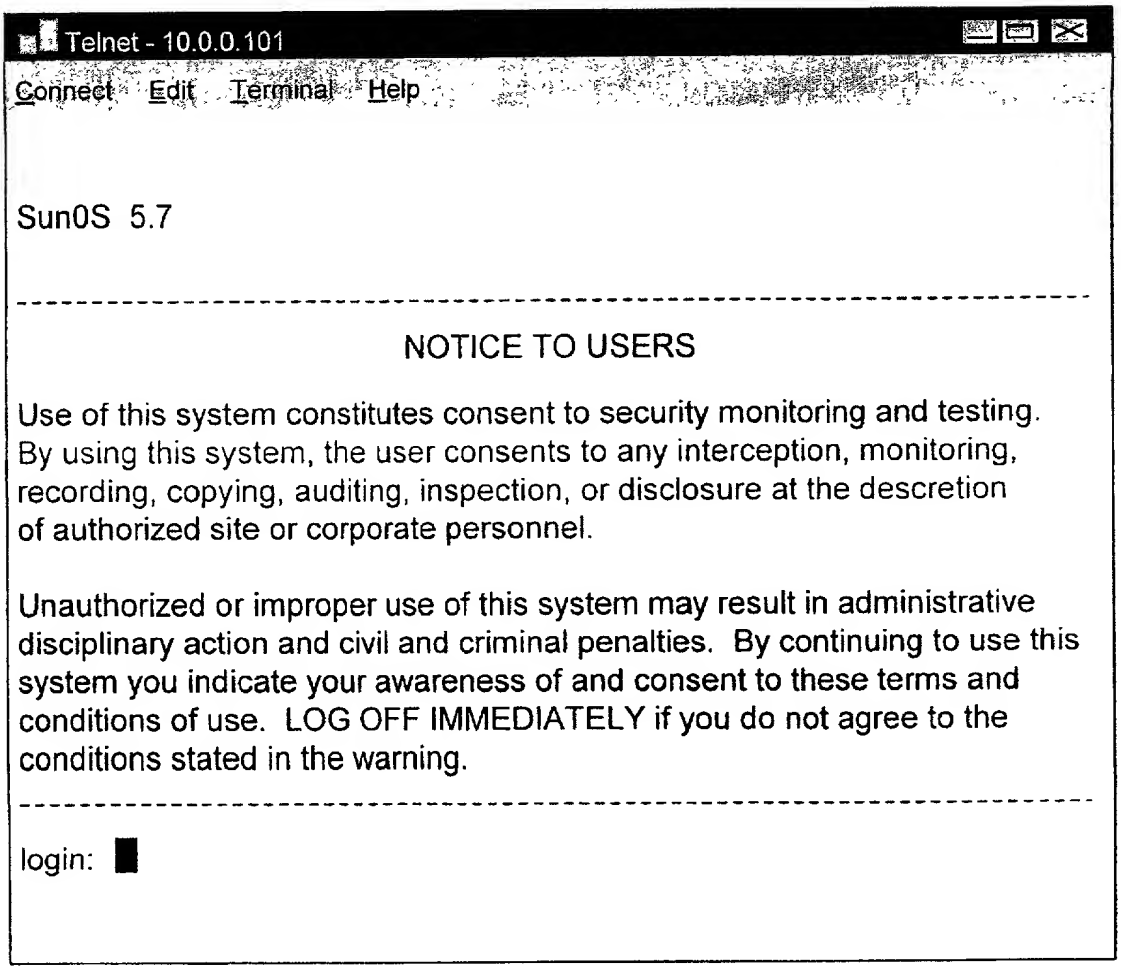
Telnet - 10.0.0.101
Connect Edit Terminal Help
SunOS 5.7
NOTICE TO USERS
Use of this system constitutes consent to security monitoring and testing. By using this system, the user consents to any interception, monitoring, recording, copying, auditing, inspection, or disclosure at the descretion of authorized site or corporate personnel.
Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in the warning.
login:

Figure 8

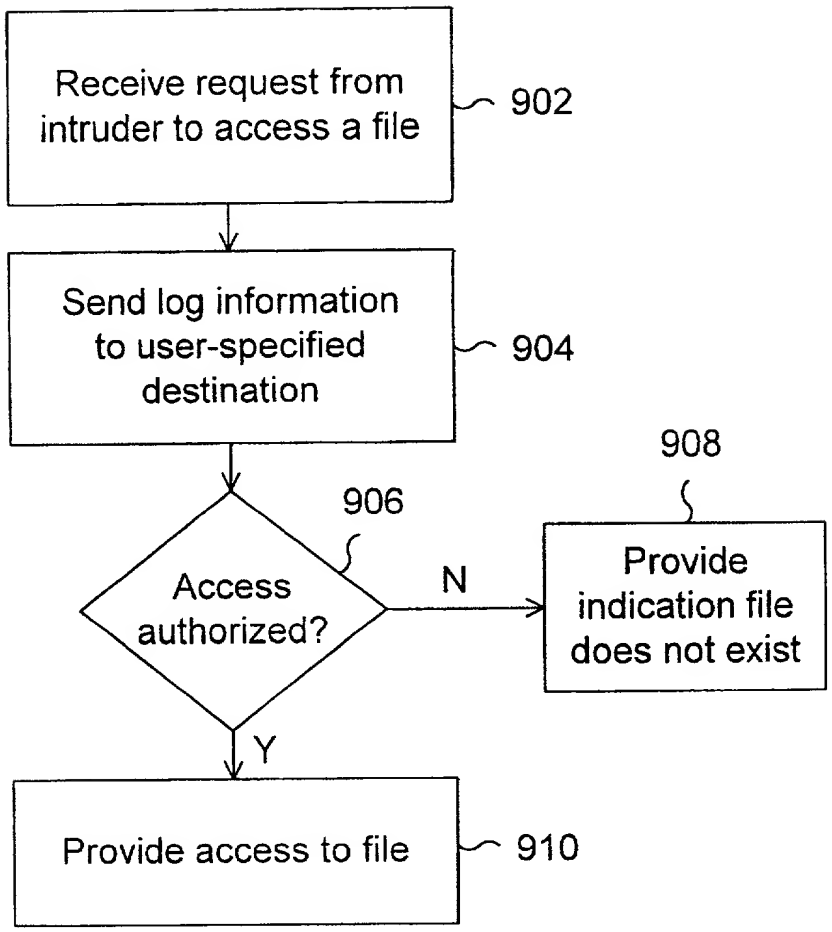
Receive request from intruder to access a file
902
Send log information to user-specified destination
904
906
Access authorized?
N
908
Provide indication file does not exist
Y
Provide access to file
910

Figure 9

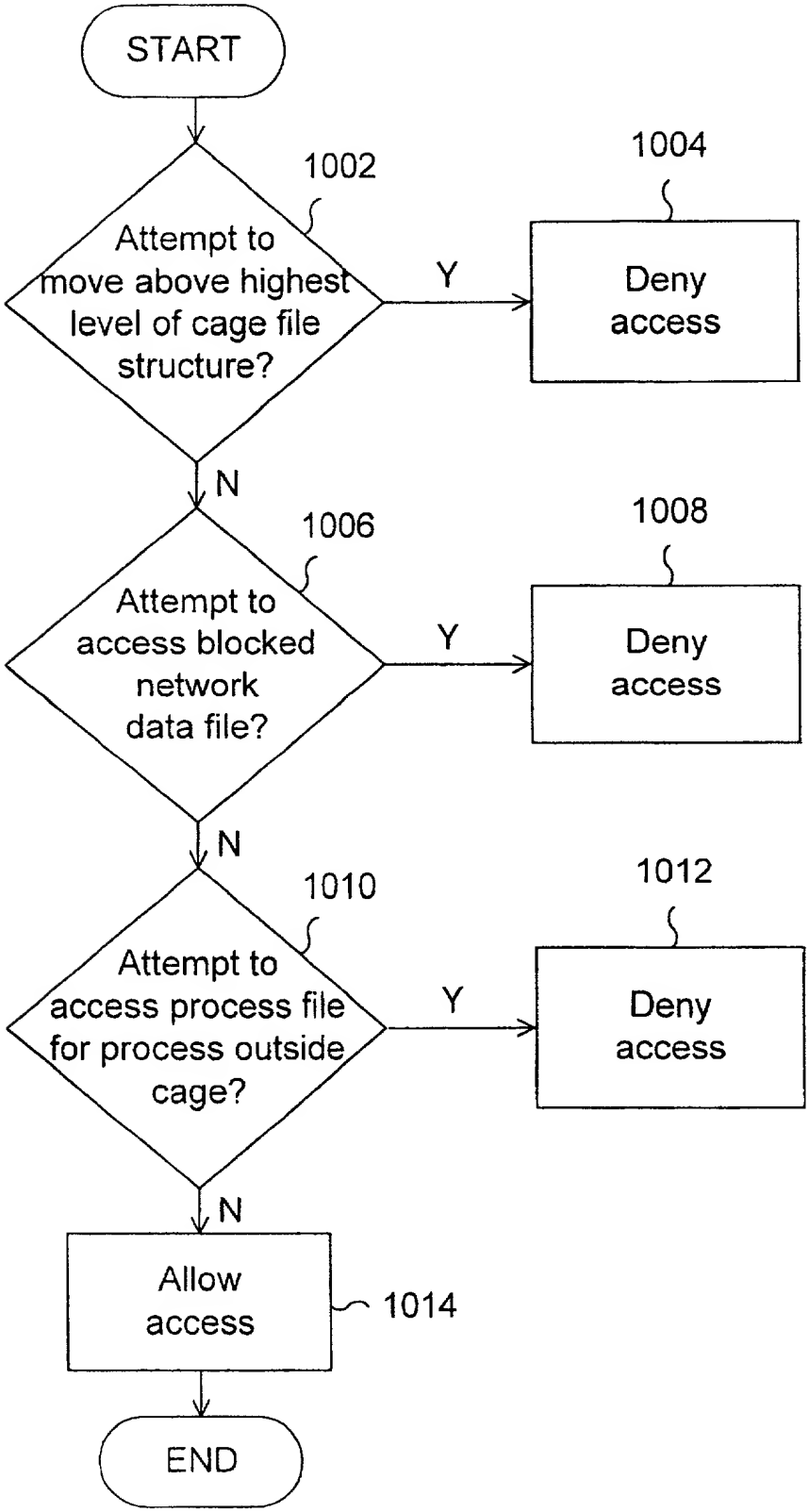
START
1002
Attempt to move above highest level of cage file structure?
Y
1004
Deny access
N
1006
Attempt to access blocked network data file?
Y
1008
Deny access
N
1010
Attempt to access process file for process outside cage?
Y
1012
Deny access
N
Allow access
1014
END

Figure 10

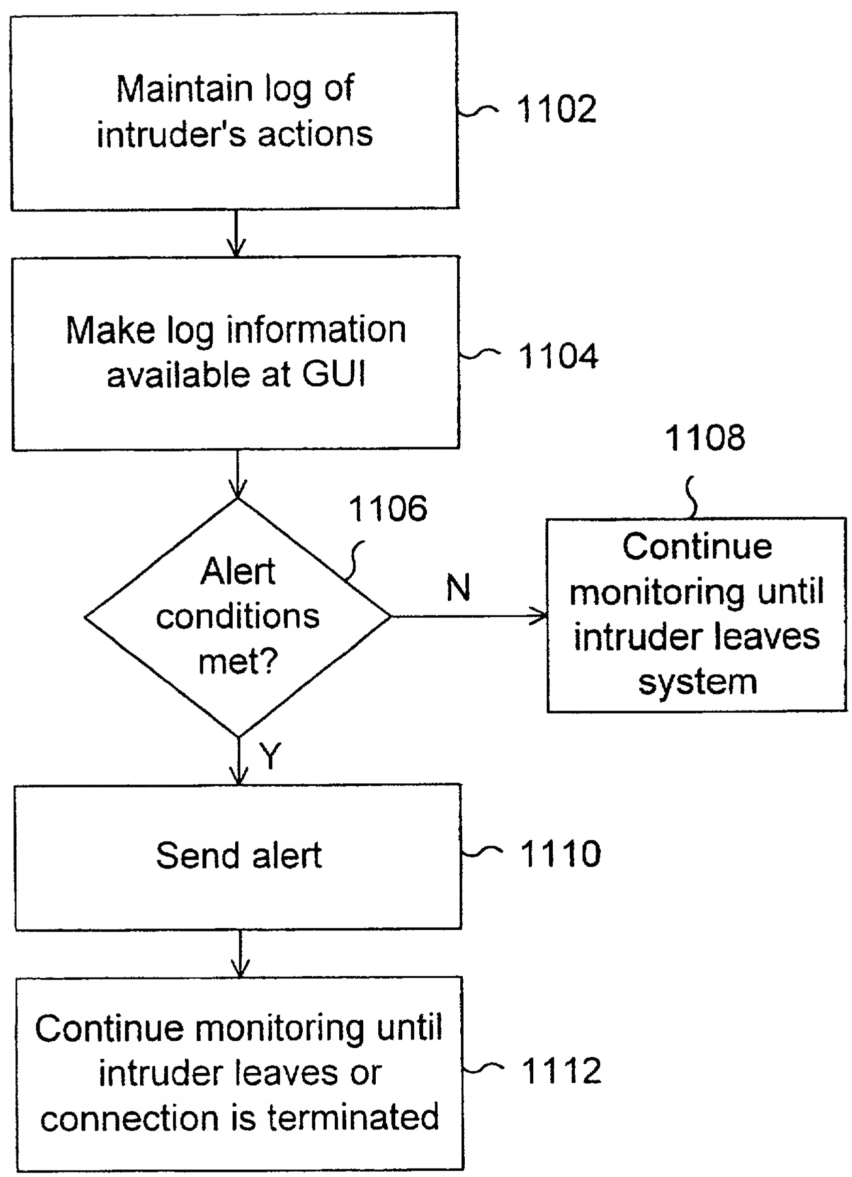
Maintain log of intruder's actions
1102
Make log information available at GUI
1104
1106
Alert conditions met?
N
1108
Continue monitoring until intruder leaves system
Y
Send alert
1110
Continue monitoring until intruder leaves or connection is terminated
1112

Figure11A

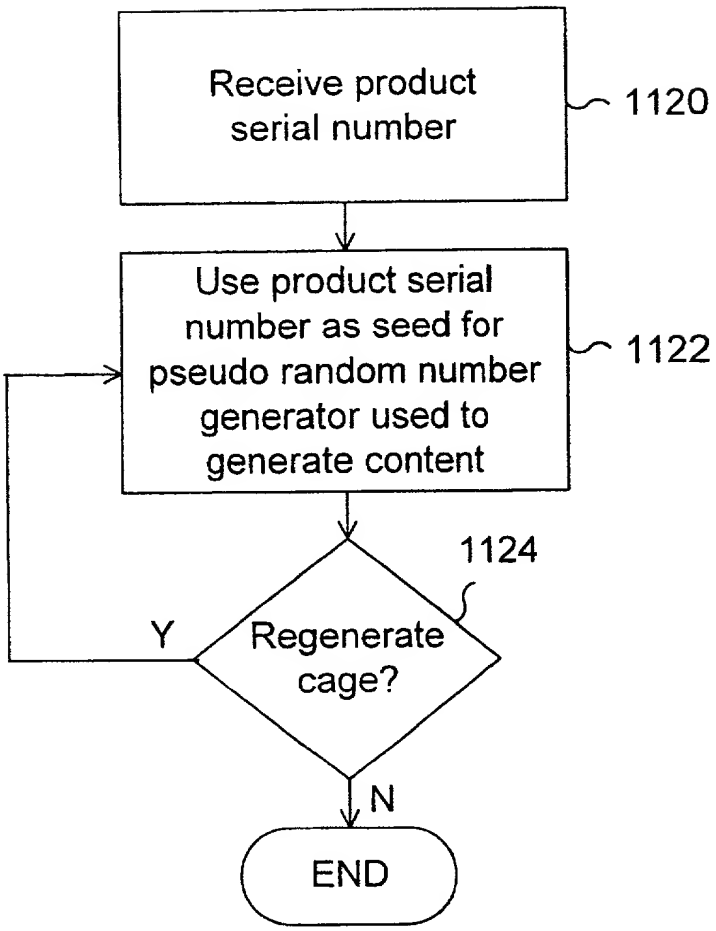
Receive product serial number
1120
Use product serial number as seed for pseudo random number generator used to generate content
1122
1124
Regenerate cage?
Y
N
END

Figure 11B

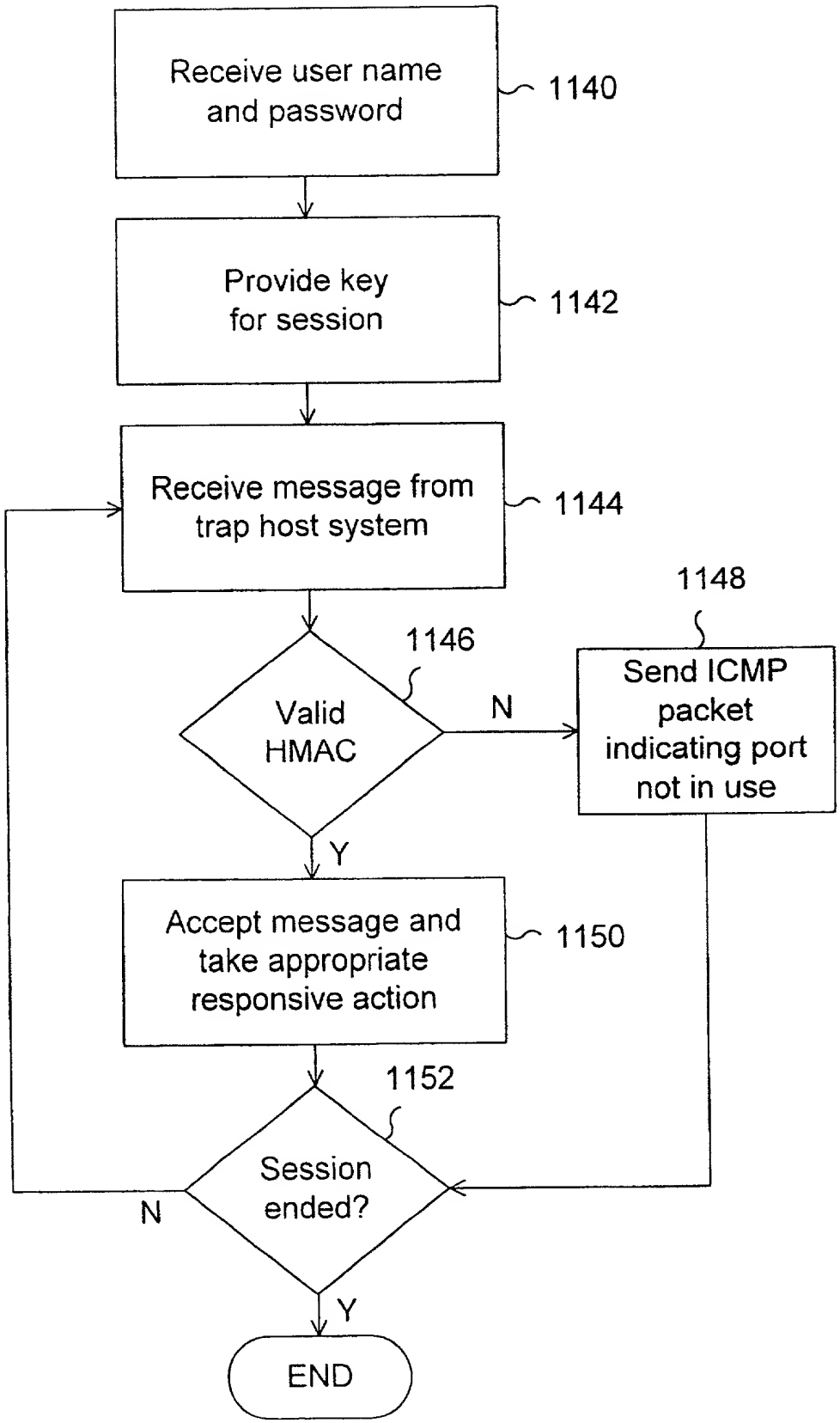
Receive user name and password
1140
Provide key for session
1142
Receive message from trap host system
1144
1148
1146
Valid HMAC
N
Send ICMP packet indicating port not in use
Y
Accept message and take appropriate responsive action
1150
1152
Session ended?
N
Y
END

Figure11C

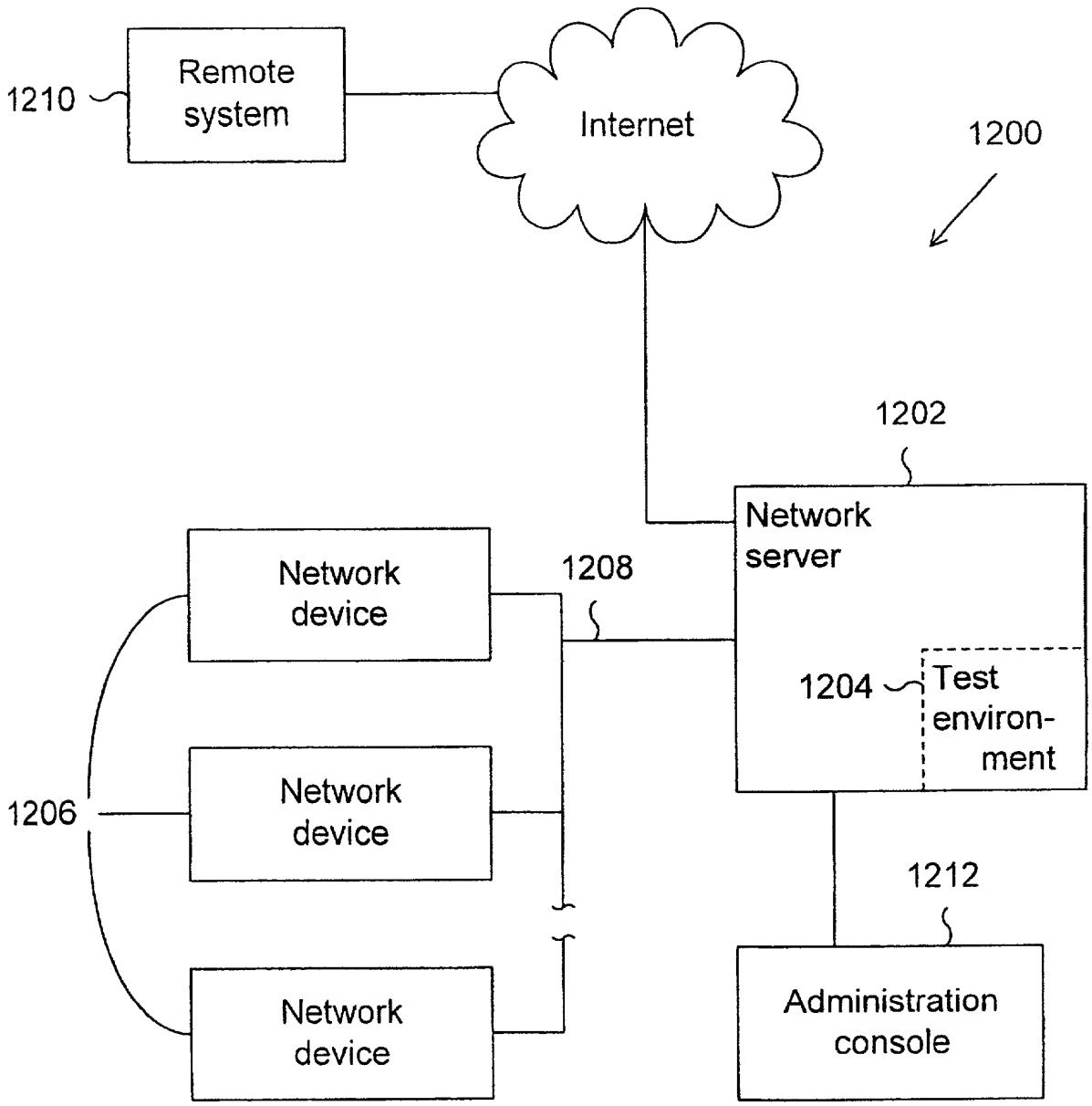
1210
Remote system
Internet
1200
1202
Network server
Network device
1208
1204
Test environ-ment
1206
Network device
1212
Network device
Administration console

Figure 12

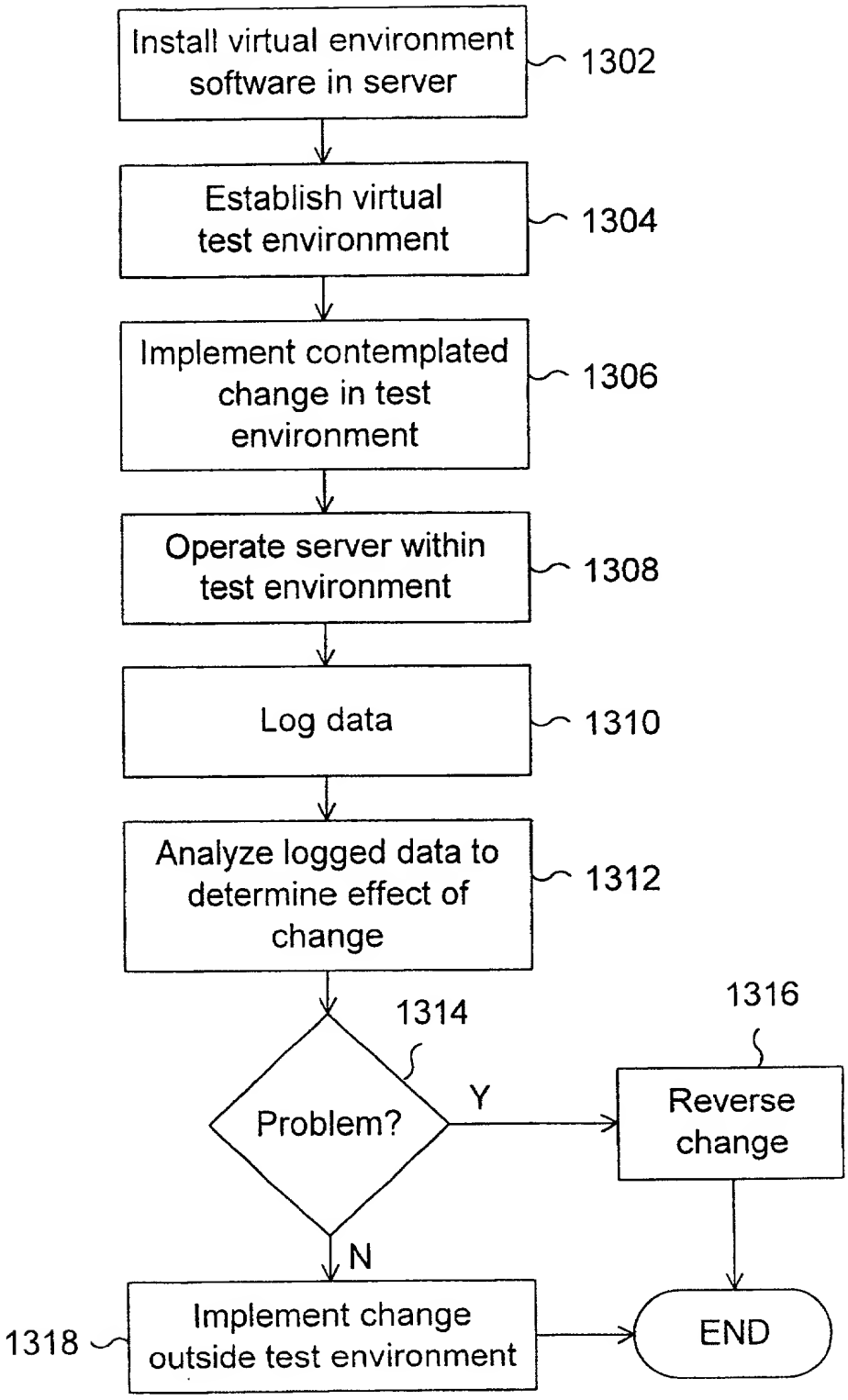
Install virtual environment software in server
1302
Establish virtual test environment
1304
Implement contemplated change in test environment
1306
Operate server within test environment
1308
Log data
1310
Analyze logged data to determine effect of change
1312
1314
Problem?
Y
1316
Reverse change
N
1318
Implement change outside test environment
END

Figure 13

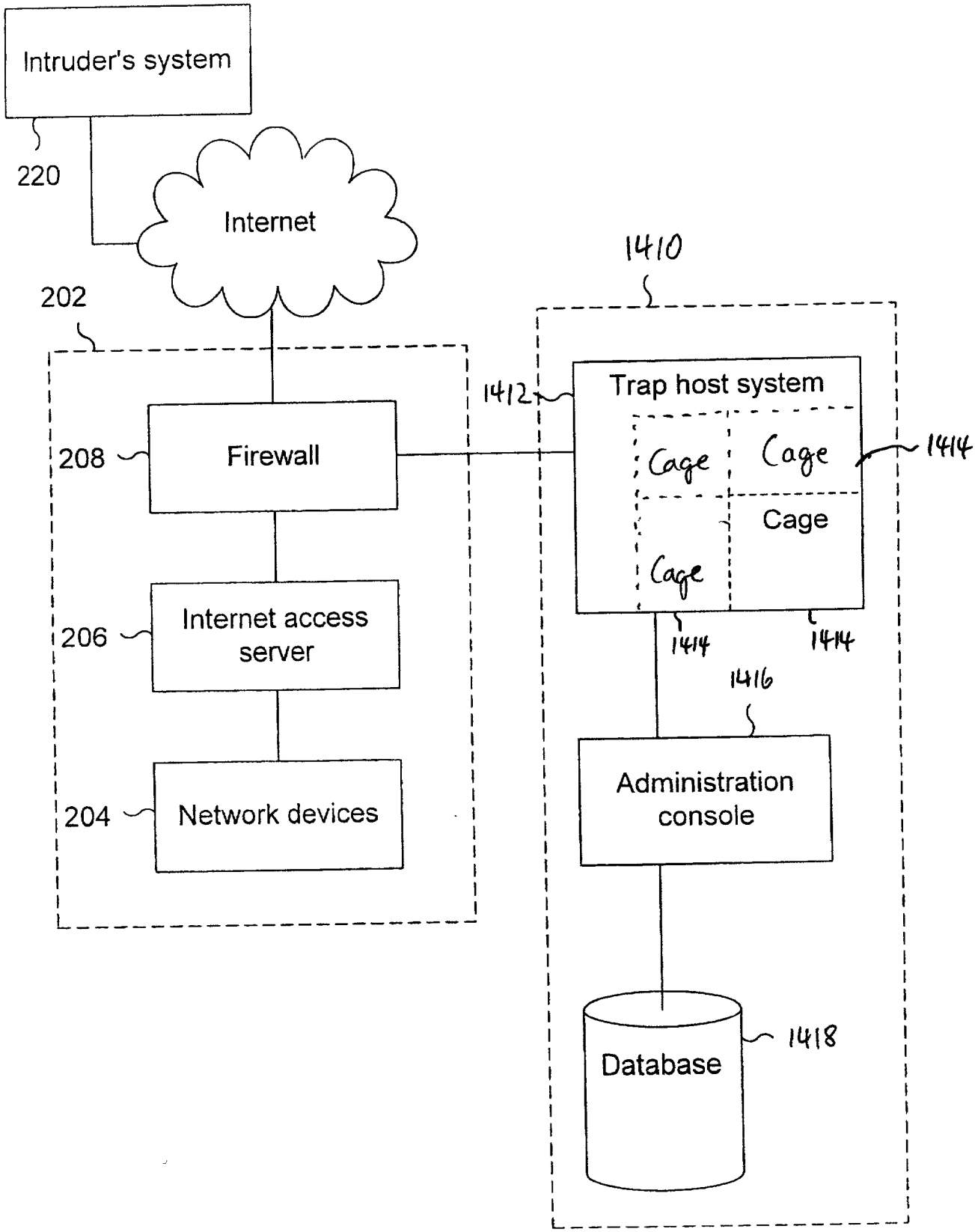
Intruder's system
220
Internet
202
1410
1412
Trap host system
208
Firewall
Cage
Cage
Cage
Cage
1414
1414
1414
206
Internet access server
1416
Administration console
204
Network devices
Database
1418

Figure 14

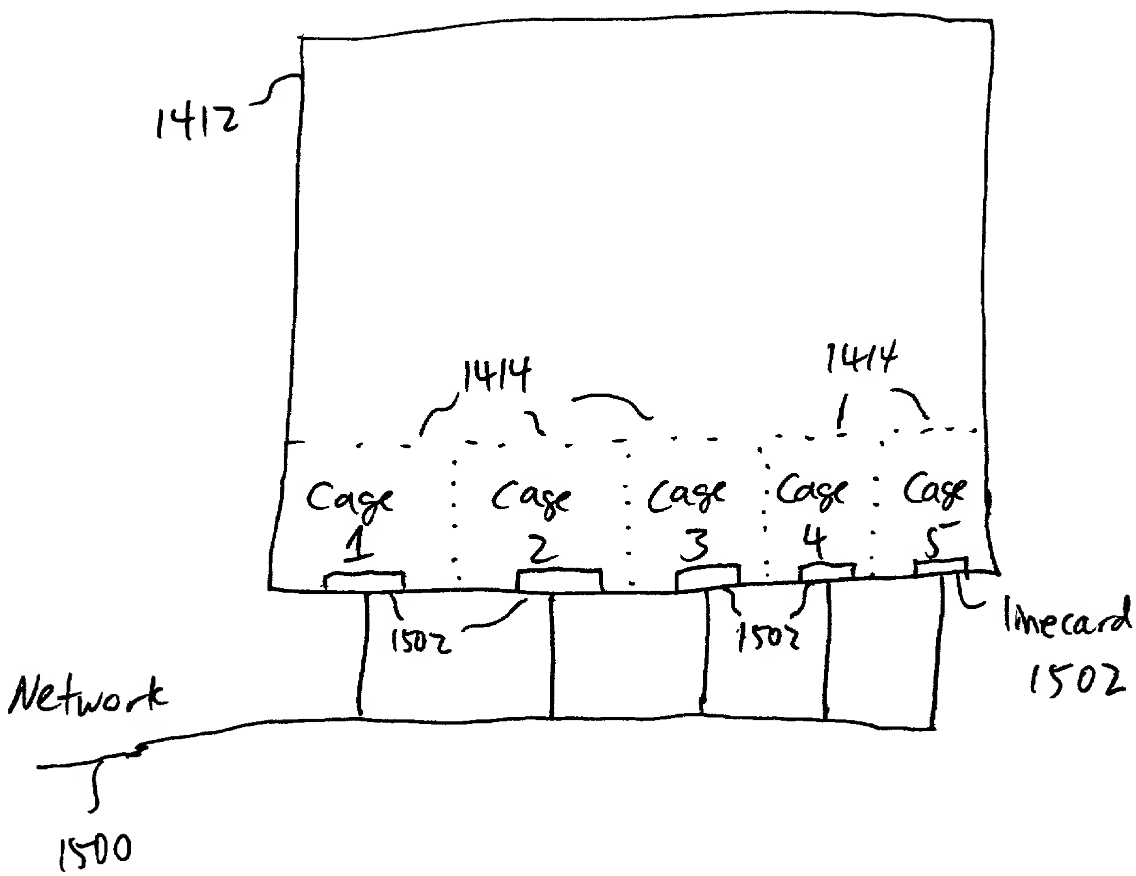
1412
1414
1414
Cage 1
Cage 2
Cage 3
Cage 4
Cage 5
1502
1502
linecard 1502
Network
1500

Figure 15

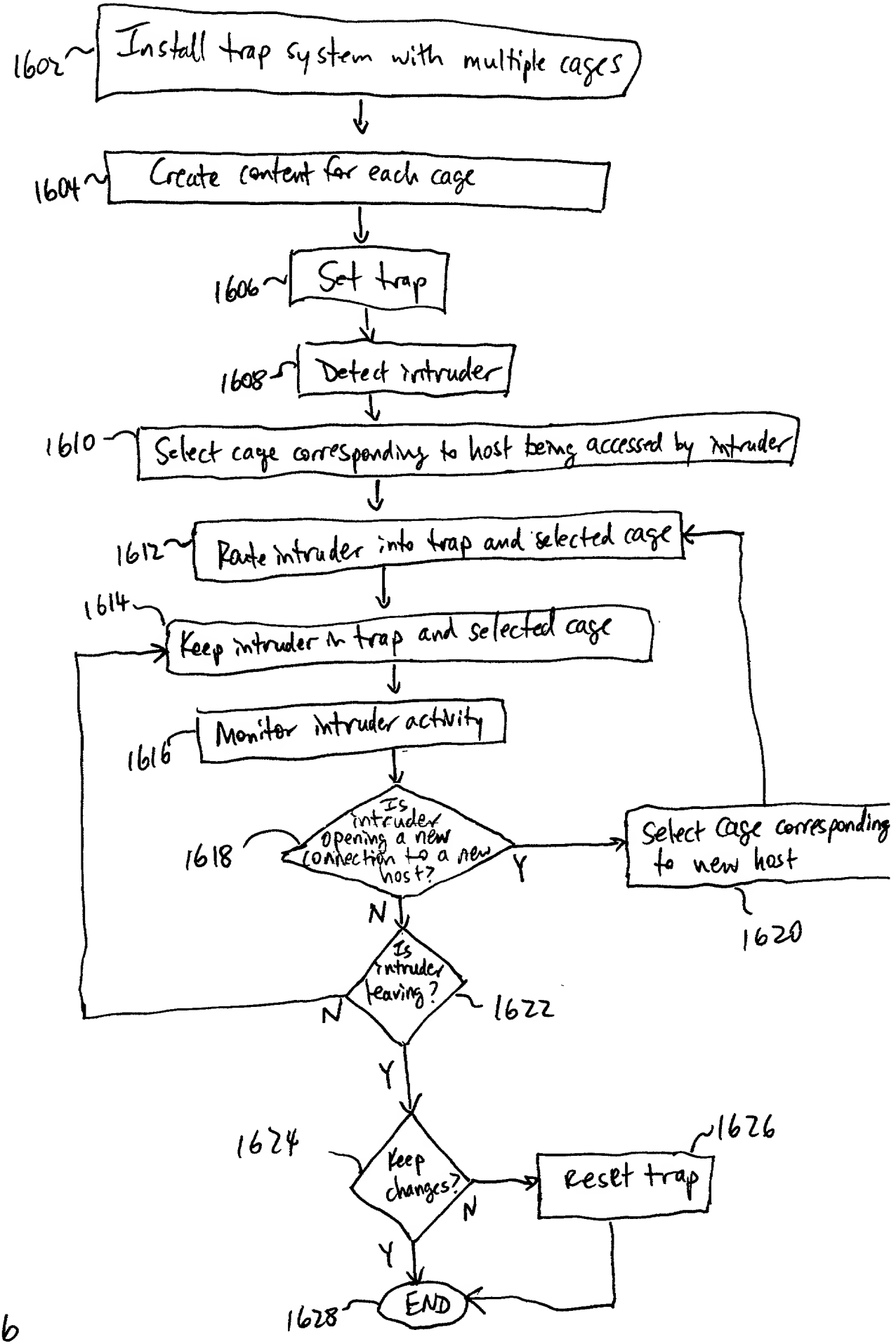

FIGURE 16

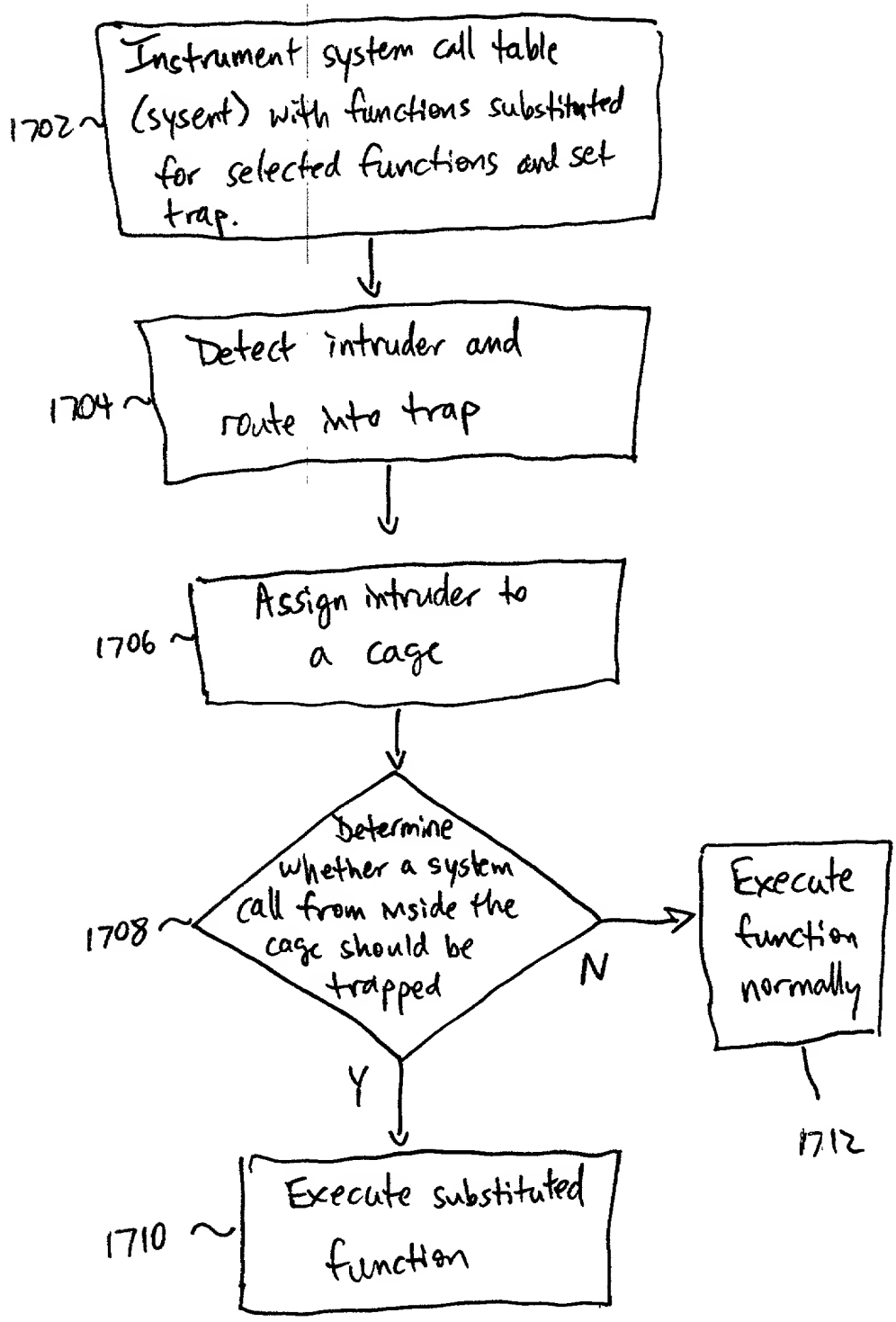
Instrument system call table (sysent) with functions substituted for selected functions and set trap.
1702
Detect intruder and route into trap
1704
Assign intruder to a cage
1706
Determine whether a system call from inside the cage should be trapped
1708
N
Execute function normally
1712
Y
Execute substituted function
1710

Figure 17

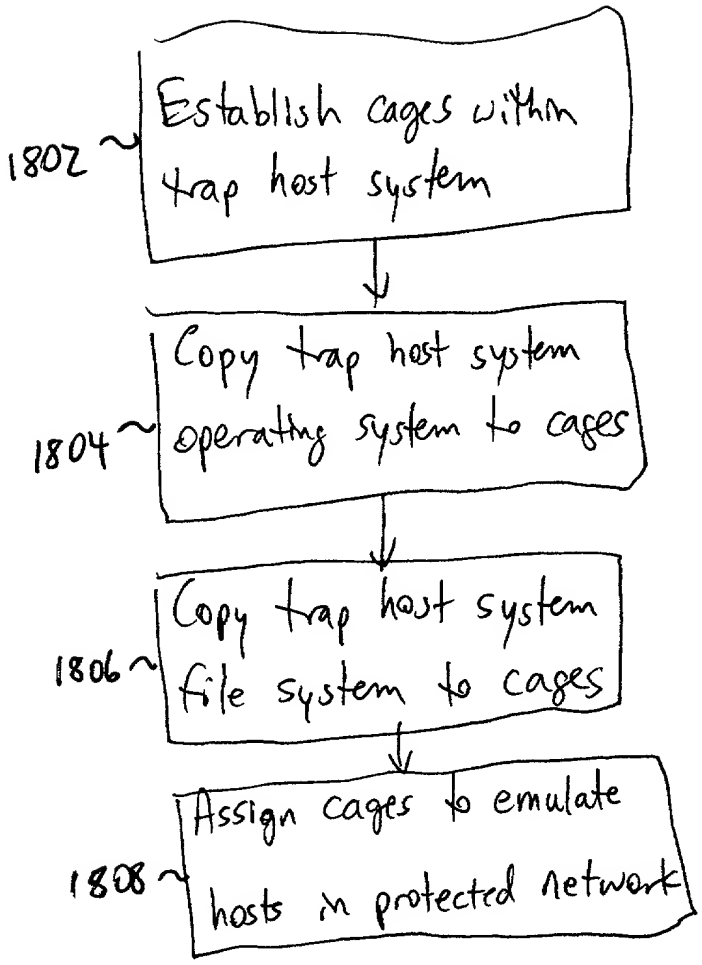
1802
Establish cages within trap host system
1804
Copy trap host system operating system to cages
1806
Copy trap host system file system to cages
1808
Assign cages to emulate hosts in protected network

Figure 18

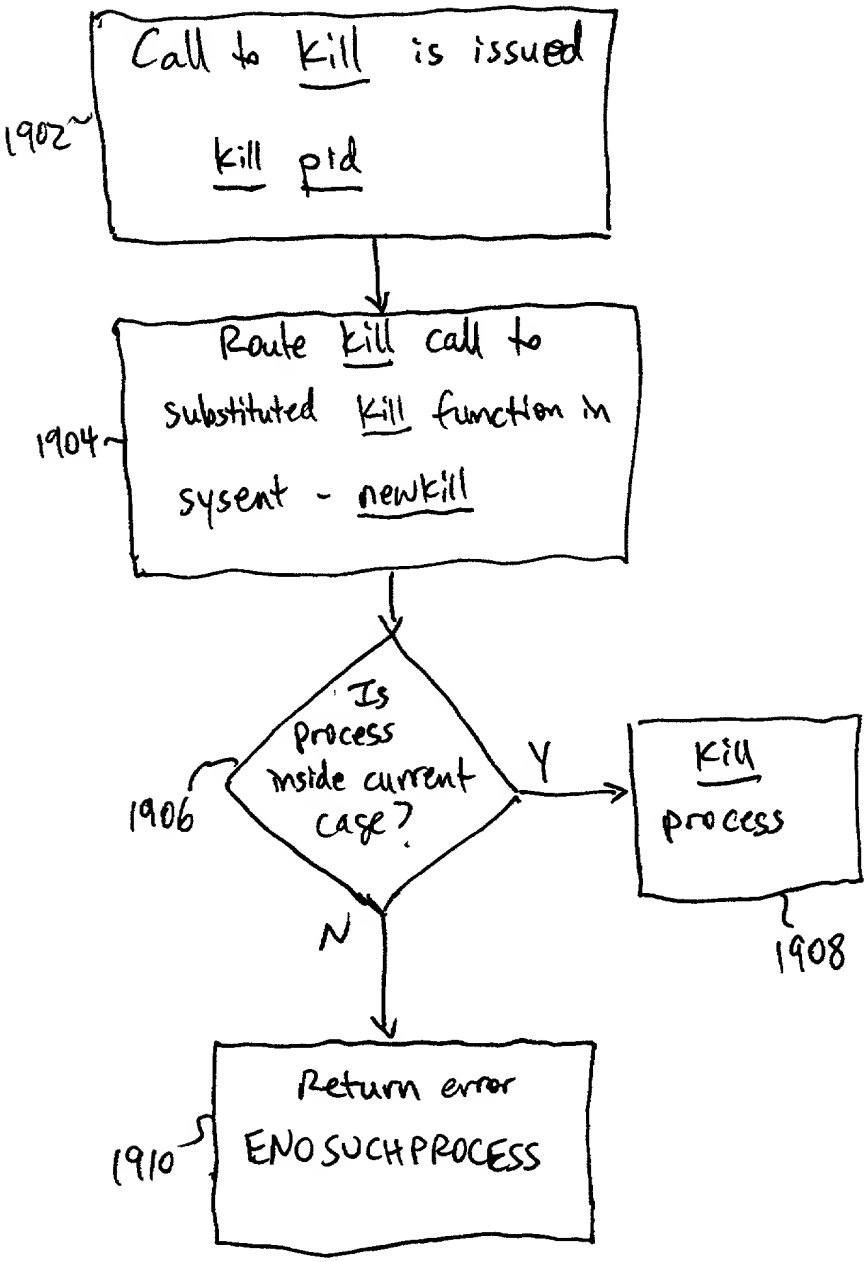
Call to kill is issued
kill pid
1902
Route kill call to substituted kill function in sysent - newkill
1904
Is process inside current case?
1906
Y
N
Kill process
1908
Return error ENOSUCHPROCESS
1910

Figure 19

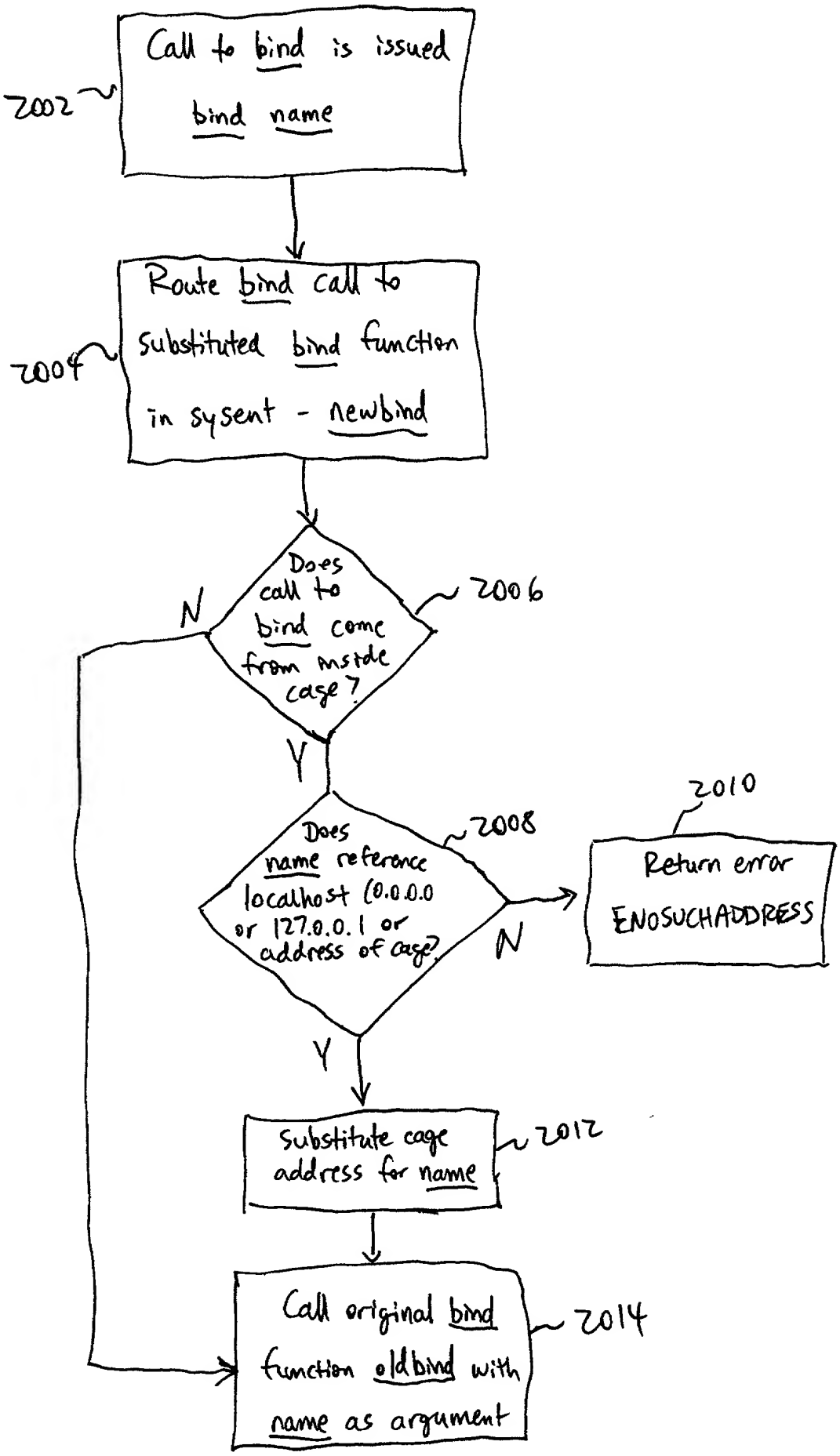
Call to bind is issued
bind name
2002
Route bind call to substituted bind function in sysent - newbind
2004
Does call to bind come from nsfde case?
2006
N
Y
Does name reference localhost (0.0.0.0 or 127.0.0.1 or address of cage?
2008
N
Y
2010
Return error ENOSUCHADDRESS
Substitute cage address for name
2012
Call original bind function oldbind with name as argument
2014

Figure 20

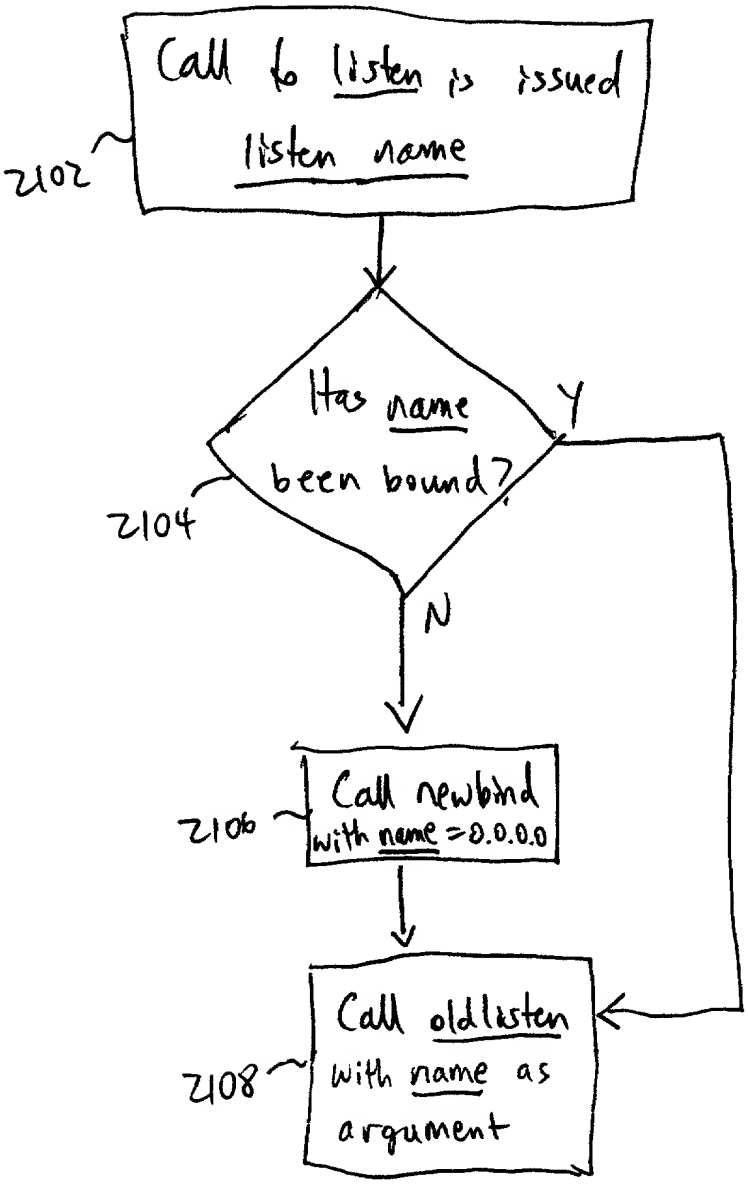
Call to listen is issued
listen name
2102
Has name been bound?
Y
N
2104
Call newbind with name =0.0.0.0
2106
Call oldlisten with name as argument
2108

Figure 21

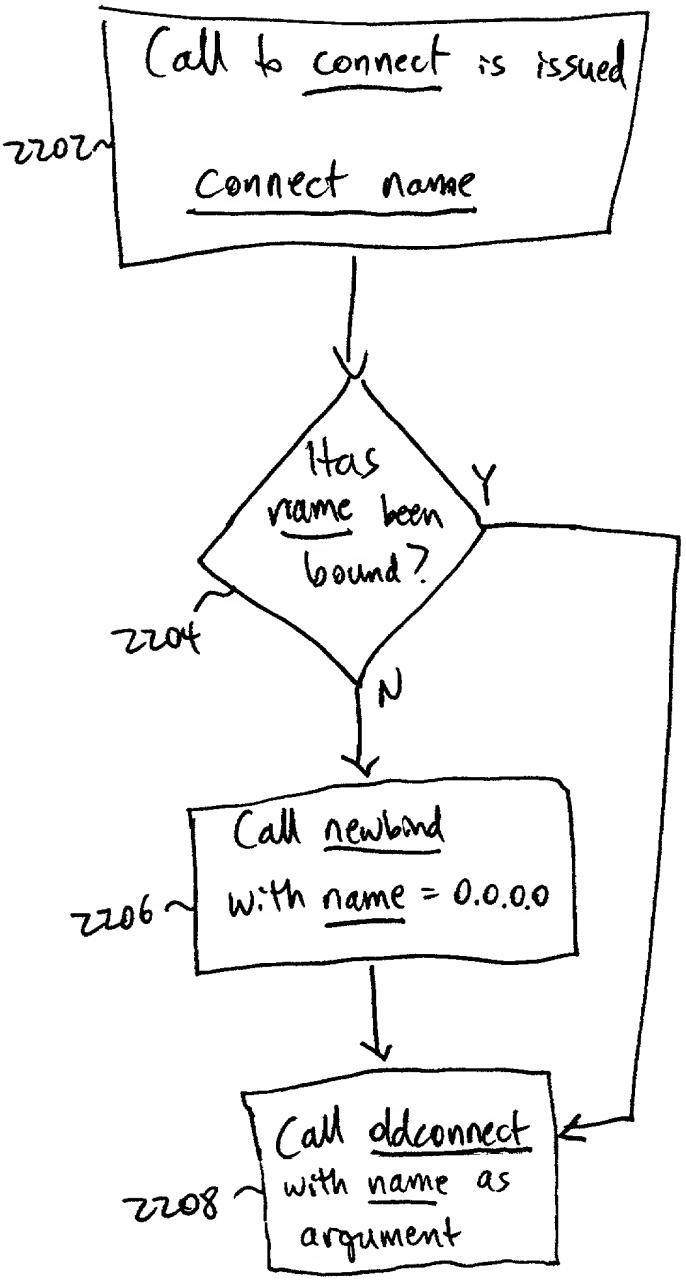
Call to connect is issued
Connect name
2202
Has name been bound?
Y
N
2204
Call newbind
with name = 0.0.0.0
2206
Call ddconnect
with name as argument
2208

Figure 22

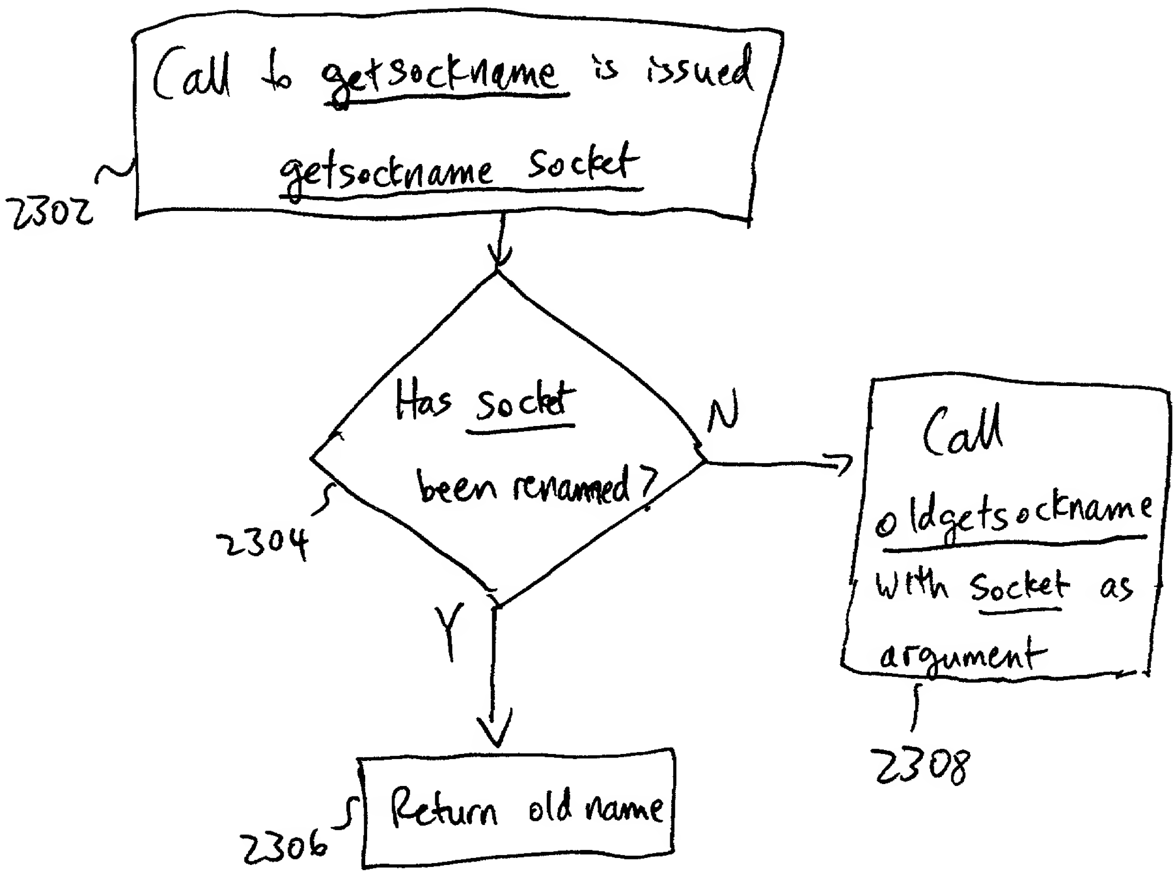

Figure 23

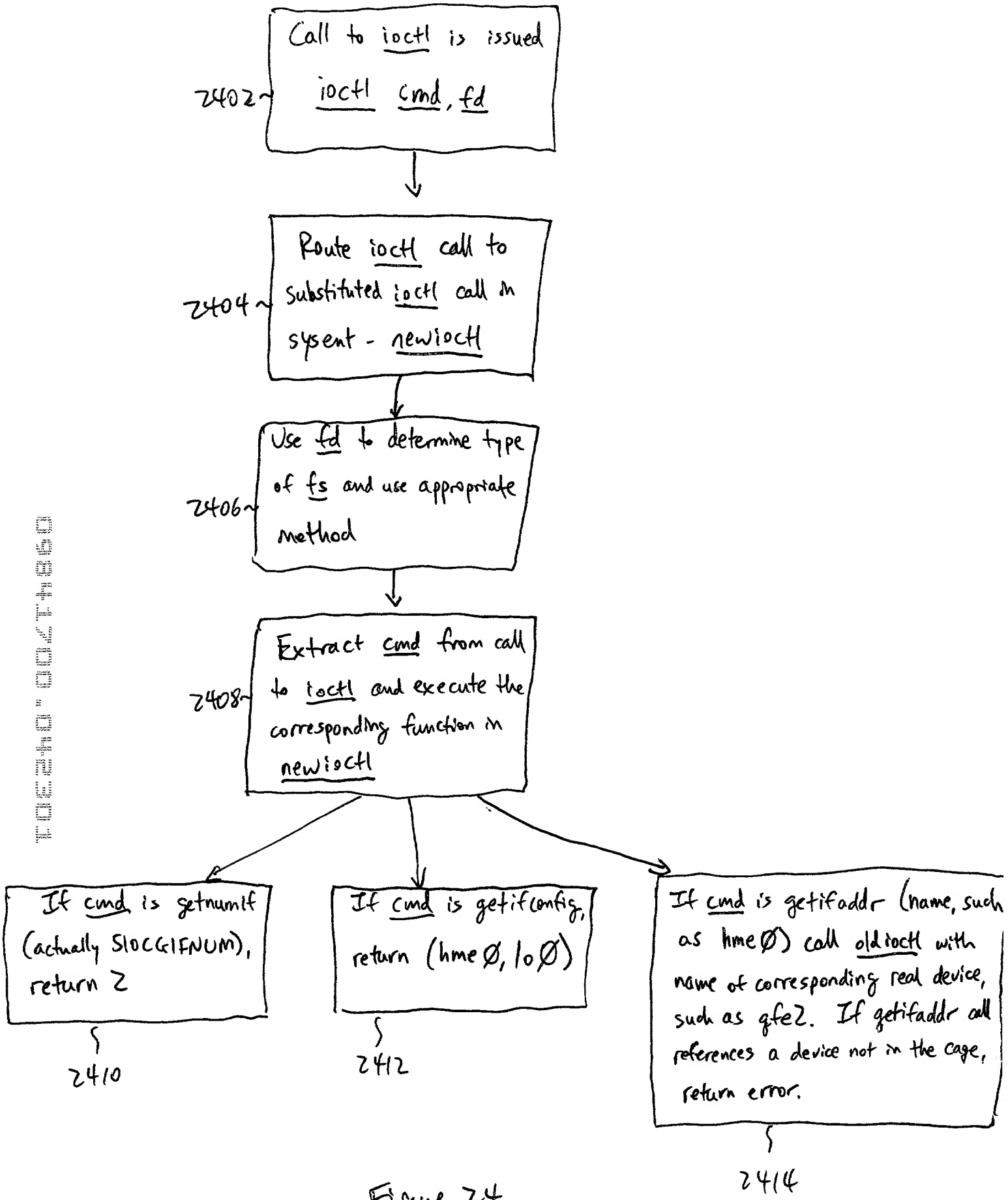
Call to ioctl is issued
ioctl cmd, fd
2402
Route ioctl call to substituted ioctl call in sysent - newioctl
2404
Use fd to determine type of fs and use appropriate method
2406
Extract cmd from call to ioctl and execute the corresponding function in newioctl
2408
If cmd is getnumif (actually SIOCGIFNUM), return 2
2410
If cmd is getifconfig, return (hme0, lo0)
2412
If cmd is getifaddr (name, such as hme0) call oldioctl with name of corresponding real device, such as qfe2. If getifaddr call references a device not in the cage, return error.
2414

Figure 24

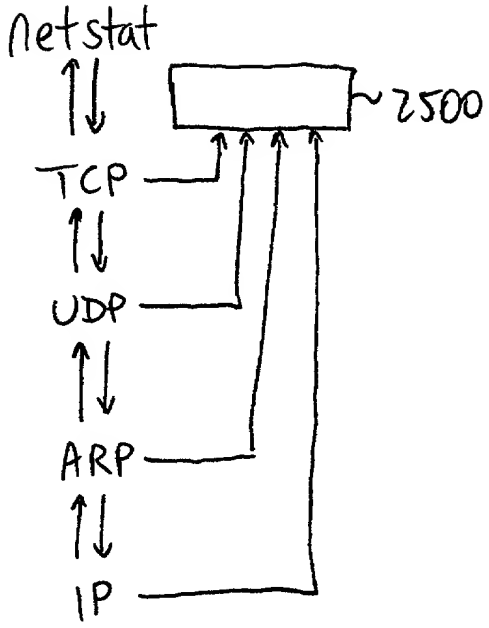

Figure 25

```
<doc>
<regexp-query>
      <name>Possible SGID Exploit</name>
      <properties>
            <priority>10</priority>
      </properties>
      <pattern>
            <next>
            <line>.*exec args=.*pid=\((\d+)\); ppid=\(\d+\); uid=\(\d+\); euid=
\(\d+\); gid=\([1-9]\d*\); egid=\(0\).*</line>
            </next>
            <next>
            <line>.*args=\([\-\w\\\/ ]+\); pid=\(\d+\); ppid=\(%1%\).*</line>
            </next>
      </pattern>
      <procmatch>
            <actionpair>
                  <line>.*args=\(([\-\w\\\/ ]+)\).*ppid=\(%1%\).*</line>
                  <action>
                        <highlight/>
                        <delete/>
                        <varop var="agg">%1%</varop>

                  </action>
            </actionpair>
      </procmatch>
      <annotation>
            <text>Possible SGID Exploit: %agg%</text>
      </annotation>
</regexp-query>
</doc>
```

Figure 26

```
<doc>
      <regexp-query>
      <name>Possible SUID Exploit</name>
      <properties>
            <priority>10< /priority>
      </properties>
      <pattern>
            <next>
            <line>.*exec args=.*pid=\((\d+)\); ppid=\(\d+\); uid=\([1-9]\d*\);
euid=\(0\).*</line>
            </next>
            <next>
            <line>.*args=\(.+\); pid=\(\d+\); ppid=\(%1%\).*</line>
            </next>
      </pattern>
      <procmatch>
            <actionpair>
                  <line>.*args=\(.+)\); pid=\(\d+\); ppid=\(%1%\).*</line>
                  <action>
                        <highlight/>
                        <delete/>
                        <varop var="agg">%1%</varop>
                  </action>
      </procmatch>
      <annotation>
            <text>Possible SUID Exploit: %agg%</text>
      </annotation>
</regexp-query>
</doc>
```

Figure 27

```
<doc>
<regexp-query>
      <name>All Processes</name>
      <properties>
            <priority>10</priority>
      </properties>
      <pattern>
            <next>
            <line>.*proclog.*args=\(([\-\.\w\\\/ ]+)\).*</line>
            </next>
      </pattern>
      <procmatch>
            <actionpair>
                  <line>.*args=\(([\-\.\w\\\/ ]+)\).*</line>
                  <action>
                        <highlight/>
                        <delete/>
                        <varop var="agg">%1%</varop>
                  </action>
            </actionpair>
      </procmatch>
      <annotation>
            <text>Process started: %agg%</text>
      </annotation>
</regexp-query>
</doc>
```

Figure 28

```
<doc>
<regexp-query>
      <name>Find Processes...</name>
      <properties>
            <priority>10</priority>
      </properties>
      <args>
            <args>.+</args>
            <pid>\d+</pid>
            <ppid>\d+</ppid>
            <uid>\d+</uid>
            <euid>\d+</euid>
            <gid>\d+</gid>
            <egid>\d+</egid>
      </args>
      <pattern>
            <next>
            <line>.*args=\(%args%\); pid=\(%pid%\); ppid=\(%ppid%\);
uid=\(%uid%\); euid=\(%euid%\); gid=\(%gid%\); egid=\(%egid%\).*</line>
            </next>
      </pattern>
      <procmatch>
            <actionpair>
                  <line>.*args=\((.+)\); pid.*</line>
                  <action>
                        <highlight/>
                        <delete/>
                        <varop var="agg">%1%</varop>
                  </action>
            </actionpair>
      </procmatch>
      <annotation>
            <text>Process started: %agg%</text>
      </annotation>
</regexp-query>
</doc>
```

Figure 29

```
<doc>
<regexp-query>
      <name>All Shell-spawned Processes</name>
      <properties>
            <priority>10</priority>
      </properties>
      <pattern>
            <next>
            <line>.*exec args=\(-sh\); pid=\((\d+)\).*</line>
            </next>
            <next>
            <line>.*args=\(([\-\w\\\/ ]+)\).*ppid=\(%1%\).*</line>
            </next>
      </pattern>
      <procmatch>
            <actionpair>
                  <line>.*args=\(([\-\w\\\/ ]+)\).*ppid=\(%1%\).*</line>
                  <action>
                        <highlight/>
                        <varop var="agg">%1%</varop>
                  </action>
            </actionpair>
      </procmatch>
      <annotation>
            <text>Executed from a shell: %agg%</text>
      </annotation>
</regexp-query>
</doc>
```

Figure 30

```
<doc>
<regexp-query>
      <name>Incoming Connections</name>
      <properties>
            <priority>10</priority>
      </properties>
      <pattern>
            <next>
            <line>.*incoming connection from=\(.+\).*</line>
            </next>
      </pattern>
      <procmatch>
            <actionpair>
                  <line>.*incoming connection from=\((.+):(.+)\)
to=\((.+):(.+)\).*</line>
                  <action>
                        <highlight/>
                        <delete/>
                        <varop var= "fromip">%1%</varop>
                        <varop var= "fromport">%2%</varop>
                        <varop var= "toip">%3%</varop>
                        <varop var= "toport">%4%</varop>
                  </action>
            </actionpair>
      </procmatch>
      <annotation>
            <text>Incoming Connection From IP: %fromip% (on port: %fromport%) To
IP: %toip% (on port: %toport%)</text>
      </annotation>
</regexp-query>
</doc>
```

Figure 31

```
<doc>
<regexp-query>
      <name>Keystrokes Entered</name>
      <properties>
            <priority>10</priority>
      </properties>
      <pattern>
            <next>
            <line>.*read stream data, id=\((\d+)\) data=\(.+\).*</line>
            </next>
            <next fromprev="1">
            <line>.*read stream data, id=\(%1%\) data=\(.*\\0[ad4].*\).*</line>
            </next>
      </pattern>
      <procmatch>
            <actionpair>
                  <line>.*read stream data,  id=\(%1%\) data=\((.+)\).*</line>
                  <action>
                        <highlight/>
                        <delete/>
                        <varop var="agg">%1%</varop>
                  </action>
            </actionpair>
      </procmatch>
      <annotation>
            <text>Keystrokes Entered: %agg%</text>
      </annotation>
</regexp-query>
</doc>
```

Figure 32

```
<doc>
<regexp-query>
      <name>Screen Output</name>
      <properties>
            <priority>10</priority>
      </properties>
      <pattern>
            <next>
            <line>.*write stream data, id=\((\d+)\) data=\(.+\).*</line>
            </next>
            <next fromprev="1">
            <line>.*write stream data, id=\(%1%\)
data=\(.*\\0[ad46].*\).*</line>
            </next>
      </pattern>
      <procmatch>
            <actionpair>
                  <line>.*write stream data, id=\(%1%\) data=\((.+)\).*</line>
                  <action>
                        <highlight/>
                        <delete/>
                        <varop var="agg">%1%</varop>
                  </action>
            </actionpair>
      </procmatch>
      <annotation>
            <text>Output to screen: %agg%</text>
      </annotation>
</regexp-query>
</doc>
```

Figure 33

```
<doc>
<regexp-query>
      <name>Find Monitored</name>
      <properties>
            <priority>10</priority>
      </properties>
      <args>
            <file_name>.+</file_name>
            <pid>\d+</pid>
      </args>
      <pattern>
            <next>
            <line>.*monitored file opened name=\(%file_name%\)
pid=\(%pid%\).*</line>
            </next>
      </pattern>
      <procmatch>
            <actionpair>
                  <line>.*monitored file opened name=\((.+)\)
pid=\((.+)\).*</line>
                  <action>
                        <highlight/>
                        <delete/>
                        <varop var="filename">%1%</varop>
                        <varop var="pidvar">%2%</varop>
                  </action>
            </actionpair>
      </procmatch>
      <annotation>
            <text>File Opened: %filename% (from pid: %pidvar%)</text>
      </annotation>
</regexp-query>
</doc>
```

Figure 34